



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/691,361	10/21/2003	Jeffrey Bruce Lotspiech	ARC920030093US1	1410
67232 7590 04/29/2011 CANTOR COLBURN LLP - IBM ARC DIVISION 20 Church Street 22nd Floor Hartford, CT 06103				
EXAMINER				
TRAN, ELLEN C				
ART UNIT		PAPER NUMBER		
2433				
NOTIFICATION DATE		DELIVERY MODE		
04/29/2011		ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

usptopatentmail@cantorcolburn.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JEFFREY BRUCE LOTSPIECH, KEVIN SNOW MCCURLEY,
and FLORIAN PESTONI

Appeal 2009-007061
Application 10/691,361¹
Technology Center 2400

Before JEAN R. HOMERE, JAY P. LUCAS, and JAMES R. HUGHES,
Administrative Patent Judges.

HUGHES, *Administrative Patent Judge.*

DECISION ON APPEAL

¹ Application filed October 21, 2003. The real party in interest is International Business Machines Corp. (Br. 1.)

STATEMENT OF THE CASE

Appellants appeal from the Examiner's rejection of claims 1, 4, 6-8, 11, 13-15, 98, and 99 under authority of 35 U.S.C. § 134(a). Claims 2, 3, 5, 9, 10, 12, 17, 18, 24, and 25 have been canceled. Claims 16, 19-23, and 26-97 have been withdrawn. The Board of Patent Appeals and Interferences (BPAI) has jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Appellants' Invention

The invention at issue on appeal relates to a system and method for protecting content from unauthorized use or distribution by securely removing electronic devices within a network. (Spec. ¶¶ [0001], [0019].)²

Representative Claims

Independent claim 1 and dependent claim 98 further illustrate the invention, and are reproduced below with the key disputed limitations emphasized:

1. A method for securely removing a device from at least one of a plurality of devices in a network while protecting a content from unauthorized use or distribution, the method comprising:

calculating an encryption key for the protected content in the network, based at least in part on a list of the plurality of devices in the network;

tentatively marking the device for removal, by modifying the list of the plurality of devices in the network, wherein the

² We refer to Appellants' Specification ("Spec."), and Appeal Brief ("Br.") filed March 14, 2008. We also refer to the Examiner's Answer ("Ans.") mailed May 23, 2008.

list of the plurality of devices is included in an authorization table;

the device marked for removal automatically acknowledging the removal;

automatically recording the removal of the device in the authorization table;

recalculating the encryption key for all the devices remaining in the network and the protected content, using the modified list; and the authorization table; and

reencrypting the protected content with the recalculated encryption key.

98. The method of claim 1 wherein:

calculating the encryption key includes calculating the encryption key in response to a management key from a key management block, a binding ID associated with each of the devices on the list and a hash of an authorization table listing authorized devices.

References

The Examiner relies on the following references as evidence in support of the rejections:

Xu	US 6,965,883 B2	Nov. 15, 2005 (filed Feb 20, 2002)
----	-----------------	---------------------------------------

International Business Machines Corp., *IBM Response to DVB-CPT Call for Proposals for Content Protection & Copy Management: xCP Cluster Protocol*, pp. 2, 6 (October 19, 2001) (“IBM Oct. 2001”).

Rejection on Appeal

The Examiner rejects claims 1, 4, 6-8, 11, 13-15, 98, and 99 under 35 U.S.C. § 103(a) as being unpatentable over the combination of IBM Oct. 2001 and Xu.

ISSUES

Based on our review of the administrative record, Appellants' contentions, and the Examiner's findings and conclusions, the pivotal issues before us are as follows:

1. Does the Examiner err in finding IBM Oct. 2001 and Xu would have taught or suggested "recalculating the encryption key for all the devices remaining in the network and the protected content, using the modified list; and the authorization table" as recited in Appellants' claim 1?
2. Does the Examiner err in finding IBM Oct. 2001 and Xu would have taught or suggested "calculating the encryption key includes calculating the encryption key in response to . . . a hash of an authorization table listing authorized devices" as recited in Appellants' claim 98?

FINDINGS OF FACT (FF)

We adopt the Examiner's findings in the Answer and Final Office Action as our own, except as to those findings that we expressly overturn or set aside in the Analysis that follows. We also add the following factual findings:

IBM Oct. 2001 Reference

1. IBM describes a copy protection system for home networks that allows devices to be securely added to the network. The system extends

the broadcast encryption techniques used for protection of content stored on portable media to the networked environment, developing a system that allows consumers to seamlessly access content within their home and beyond, while at the same time protecting the rights of content owners. IBM's "xCP Cluster Protocol" binds protected content to a dynamic cluster of networked recording and playback devices, such that the content can be managed on those devices under a single protection scheme independent of particular storage or transmission interfaces and protocols.

(IBM Oct. 2001 at 2 (bottom middle) (emphasis omitted); *see* p. 5, Figure 1.)

2. IBM describes the copy protection system as including a number of encryption keys – a media key calculated from a media key block (pp. 3-6), a binding key (p. 6), and title keys (p. 6). "Each piece of content or each content stream in the home is protected with a [title] key," and "[e]ach title key is encrypted with the [binding] key." "To play content, a device reads the encrypted title key embedded in the content file and decrypts it with the binding key. Then, with the title key, the device decrypts the content itself." (p. 6 (middle).) The binding key "is calculated as the cryptographic hash of three quantities: the media key, the network's binding ID, and network's authorization table." (*Id.*) "The third element,

the network authorization table, is a simple file. However, by including it in the binding key calculation, it prevents a man-in-the-middle on the network from isolating devices from one another, for the purpose of avoiding limitations on the number of devices allowed in a network.” (p. 6 (bottom middle).) The authorization table includes all of the devices in the home network or cluster. (See pp. 5-6 (all devices are peers/severs that can authorize other devices, and each device calculates the binding key using the authorization table); 10 (authorization table is an ASCII file containing all the acknowledged authorization messages for the cluster, devices calculate the same hash for the same list of authorizations).

3. IBM explains that “the binding key will change whenever: [(1)] A new device is introduced into the home (changing the authorization table), or [(2)] A new media key block is brought in from an external source.” (p. 6 (bottom middle).) IBM also explains that “[e]very time the binding key changes, all devices in the cluster shall re-encrypt all title keys.” (*Id.*)

Xu Reference

4. Xu describes a system providing multicast (streamed) data to a user connected to a multicast session. The user specifies the start and end time of the session, and may extend, shorten, or terminate a session. (Col. 1, ll. 14-21, 48-53; col. 3, ll. 44-67.) Xu further describes providing a key (decryption key) when a user joins a session, and updating the key when a user terminates a session or a session expires:

Group membership management 122 maintains the group membership information for every terminal on the same multicast link and is responsible for determining the join status of each terminal. Multicast security unit 123 is responsible for

sending decryption key 118 to user terminal 110. . . . Multicast security unit 123 sends decryption key 118 when the user initially joins a multicast session. Multicast security unit 123 updates decryption key 118 either when another multicast user terminates the session or at discrete time intervals.

(Col. 7, ll. 5-17; Fig. 1B; *see* col. 11, ll. 22-45; col. 12, l. 45 to col.13, l. 2; col. 13, l. 45 to col. 14, l. 35; Figs. 2A-2D.)

ANALYSIS

Appellants argue claims 1, 4, 6-8, 11, and 13-15 together as a group with respect to the Examiner's § 103 rejection of the claims. (Br. 3-5.) Appellants also argue dependent claims 98 (dependent on claim 1) and 99 (dependent on claim 8) with respect to the Examiner's § 103 rejection of the claims. (Br. 5.) Therefore, we select independent claim 1 and dependent claim 98 as representative of Appellants' arguments and groupings with respect to the Examiner's obviousness rejections. 37 C.F.R. § 41.37(c)(1)(vii). *See In re Nielson*, 816 F.2d 1567, 1572 (Fed. Cir. 1987). We have considered only those arguments that Appellants have actually raised in their Brief. Arguments that Appellants could have made but chose not to make in their Brief have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

Appellants have the opportunity on appeal to the Board of Patent Appeals and Interferences (BPAI) to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) (citing *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)). The Examiner sets forth a detailed explanation of a reasoned conclusion of obviousness in the Examiner's Answer with respect to each of Appellants' claims (Ans. 3-9), and in particular claims 1 (Ans. 3-4, 6-8) and 98 (Ans. 5, 8-9). Therefore,

we look to the Appellants' Brief to show error in the proffered reasoned conclusions. *See Kahn*, 441 F.3d at 985-86.

*Arguments Concerning the Examiner's Rejection of
Representative Claim 1 Under § 103*

The Examiner rejects Appellants' independent claim 1 as being obvious over the combination of IBM Oct. 2001 and Xu. (Ans. 3-4.) Representative claim 1, in relevant part, recites "recalculating the encryption key for all the devices remaining in the network and the protected content, using the modified list; and the authorization table" when a device has been removed from the network. (Br. 7, claim 1.) Specifically, the Examiner finds that IBM Oct. 2001 teaches a binding key and tile key (Ans. 3), and recalculating the binding key whenever a new device is introduced into the home network (changing the authorization table) (Ans. 4). The Examiner further Xu teaches updating a decryption key when a user terminal terminates a multicast session. (Ans. 4.)

Appellants, on the other hand, contend that "[n]either IBM Oct. 2001 nor Xu teaches or suggests [the] feature" of "recalculating the encryption key for all the devices remaining in the network and the protected content, using the modified list; and the authorization table." (Br. 3) Specifically, Appellants contend that IBM does not teach: (1) removing a device from the network, or (2) recalculating the encryption key "using the modified list; and the authorization table." (Br. 4.) Appellants further contend that Xu does not teach "that a device is marked for removal or that the device is being removed from the network . . . [because the] device has terminated a session, not been removed from the network." (Br. 4.)

Based on the record before us, we do not find error in the Examiner's obviousness rejection of Appellants' claim 1. We also agree with the Examiner that: (1) IBM Oct. 2001 would have taught or at least suggested recalculating the encryption key for the devices in the network and the protected content utilizing using a modified authorization table including a list of devices; and (2) Xu would have taught disconnecting/terminating a user terminal connection (a connected device) from a multicast session and updating an encryption key in response to the termination. (FF 1-4.)

As detailed in the Findings of Fact section *supra*, IBM Oct. 2001 describes a network copy protection system that securely adds devices to the network, and updates a binding key when the authorization table changes. (FF 1-3.) IBM Oct. 2001 also describes the authorization table as containing a list of each authorized device in the network. (FF 2.) Xu describes updating an encryption key when a device terminates a multicast session connection. (FF 4.) Accordingly, we find that IBM Oct. 2001 would have at least suggested updating an authorization table when a device is removed from the network (instead of being added), and updating a binding key in response to the authorization table changing. Xu reinforces this suggestion by teaching updating an encryption key when a user terminal terminates a connection to (a device is removed from) a multicast session. In both cases the purpose would be to prevent circumvention or unauthorized devices (e.g., with respect to XU, devices that are no longer being charged for the multicast service) from accessing content on the network. We also find that IBM Oct. 2001 would have at least suggested recalculating an encryption key using an authorization table including the modified list of authorized devices in the network.

Thus, we find that IBM Oct. 2001 and Xu would have taught or suggested the disputed feature – “recalculating the encryption key for all the devices remaining in the network and the protected content, using the modified list; and the authorization table” – of Appellants’ representative claim 1 to one of ordinary skill in the art at the time of Appellants’ invention, rendering claim 1 obvious. We find Appellants’ contrary arguments unavailing. Appellants’ arguments are not commensurate with the scope of Appellants’ claim. Claim 1 does not recite or require that the list and authorization table cannot be combined (contain different information), in fact Appellants’ claim recites the opposite that “the list of the plurality of devices is included in an authorization table.” Further, Appellants attempt to attack the references individually, instead of addressing the combination of references. See *In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986) (noting that one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references) (citing *In re Keller*, 642 F.2d 413, 425 (CCPA 1981)). Also, Appellants failed to file a Reply Brief to rebut the findings and responsive arguments made by the Examiner in the Answer. Therefore, we find that Appellants do not provide any persuasive evidence or argument that the combination of IBM Oct. 2001 and Xu would not have taught or suggested the disputed features of Appellants’ claim.

Appellants do not separately argue independent claim 8, dependent claims 4, 6, and 7 (dependent on claim 1), or dependent claims 11 and 13-15 (dependent on claim 8) (*supra*), all of which include limitations of similar scope to the disputed limitations discussed with respect to claim 1. It follows that Appellants do not persuade us of error in the Examiner’s

obviousness rejection of claims 1, 4, 6-8, 11, and 13-15, and we affirm the Examiner's rejection of these claims.

*Arguments Concerning the Examiner's Rejection of
Representative Claim 98 Under § 103*

The Examiner rejects Appellants' dependent claim 98 as being obvious over the combination of IBM Oct. 2001 and Xu. (Ans. 5, 8-9.) Representative claim 98, in relevant part, recites "calculating the encryption key includes calculating the encryption key in response to . . . a hash of an authorization table listing authorized devices." (Br. 8, claim 98.) Specifically, the Examiner finds that "IBM Oct. 2001 teaches calculating the encryption key . . . with . . . a hash of an authorization table listing authorized devices." (Ans. 9.) Appellants contend that "[c]laims 98 and 99, however, only recite using the hash of the authorization table, not all three quantities. Thus, IBM Oct. 2001 does not teach the elements of claims 98 and 99." (Br. 5)

Based on the record before us, we do not find error in the Examiner's obviousness rejection of Appellants' claim 98. We also agree with the Examiner that IBM Oct. 2001 teaches calculating an encryption key utilizing a hash of an authorization table. (Ans. 9; FF 2.)

Thus, we find that IBM Oct. 2001 and Xu would have taught or suggested the disputed features of Appellants' representative claim 98 to one of ordinary skill in the art at the time of Appellants' invention, rendering the claim obvious. We find Appellants' contrary arguments unpersuasive. As pointed out by the Examiner, it is irrelevant that IBM Oct. 2001 also describes calculating the key using a hash of an authorization table and additional data elements (the media key and the network's binding ID). The

claim does not preclude a hash of data in addition to an authorization table. Also, Appellants failed to file a Reply Brief to rebut the findings and responsive arguments made by the Examiner in the Answer. Therefore, we find that Appellants do not provide any persuasive evidence or argument that the combination of IBM Oct. 2001 and Xu would not have taught or suggested the disputed features.

Appellants do not separately argue dependent claim 99 (*supra*), which includes the disputed limitation discussed above. It follows that Appellants do not persuade us of error in the Examiner's obviousness rejection of claims 98 and 99, and we affirm the Examiner's rejection of these claims.

CONCLUSION OF LAW

Appellants have not shown that the Examiner erred in rejecting claims 1, 4, 6-8, 11, 13-15, 98, and 99 under 35 U.S.C. § 103(a).

DECISION

We affirm the Examiner's rejection of claims 1, 4, 6-8, 11, 13-15, 98, and 99 under 35 U.S.C. § 103(a).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(v).

AFFIRMED

msc